Statement of John S. Pistole

Administrator

Transportation Security Administration

U.S. Department of Homeland Security

Before the

United States House of Representatives

Committee on Homeland Security

Subcommittee on Transportation Security

February 10, 2011

Good morning Chairman Rogers, Ranking Member Jackson Lee, and distinguished Members of the Subcommittee. I appreciate the opportunity to appear before you and this Subcommittee today to discuss the Transportation Security Administration (TSA). TSA's mission is to prevent terrorist attacks and reduce the vulnerability of the Nation's transportation system to terrorism. In meeting this mission, TSA's goal at all times is to maximize transportation protection and security in response to the evolving terrorist threat while protecting passengers' privacy and facilitating the flow of legal commerce.

In the aviation domain, TSA has implemented an effective and dynamic security system consisting of multiple layers of risk-based measures, working in concert with our international, federal, state, local, tribal, territorial and private sector partners. Our security approach begins well before a traveler arrives at an airport, with our intelligence and law enforcement partners working to detect, deter, and prevent terrorist plots before they happen, and continues all the way through the flight, providing security throughout a passenger's trip—not just at screening checkpoints.

In the surface arena, we continue to work with our partners to reduce vulnerabilities and strengthen resilience against a terrorist attack. We are working to direct grants to the most at-risk transit properties. Our Surface Security Inspectors are assisting with the development of specific security programs. And our Visible Intermodal Prevention and Response (VIPR) teams are being deployed in thousands of mass transit, maritime and highway security initiatives.

Despite all our efforts and advances in intelligence, technology, and screening processes, the threat to the U.S. transportation sector remains high. We face a committed enemy who continues to collect its own intelligence against our security measures, seeking to exploit vulnerabilities in the system. As a result, we must continue to work to stay ahead of this constantly evolving threat.

A Persistent Threat To Civil Aviation

For more than two decades, al-Qaeda and other terrorist organizations have sought to do harm to this country, and many of their plots against the United States have focused on the aviation system. It is clear that terrorist intent to strike at American targets has not diminished. We have continued to watch the threat evolve from checked baggage to hand baggage to non-metallic devices hidden on the body to air cargo. Non-metallic explosive devices are now the foremost threat to passenger airlines and it is imperative we maintain and enhance our capability to detect these threats.

One of the most salient public examples of the ongoing terrorist threat is the bombing plot by al-Qaeda in the Arabian Peninsula, which resulted in the December 25, 2009, alleged attempt by Umar Farouk Abdulmutallab to blow up an American airplane over the United States using a non-metallic explosive device that was not and could not have been discovered by a metal detector. Also, in October 2010, al-Qaeda in the Arabian Peninsula attempted to destroy two airplanes in flight using artfully concealed explosive devices hidden in cargo that highlighted the need to strengthen security across the international supply chain.

I firmly believe our best defense against these and other terrorist threats remains a risk-based, layered security approach that utilizes a range of measures both seen and unseen. This approach includes using Advanced Imaging Technology (AIT) and pat-downs to enhance and supplement the efforts of law enforcement, intelligence, and terrorist watch list checks, strengthening supply chain security, and increasing international collaboration.

Deploying Advanced Imaging Technology

After analyzing the latest intelligence and studying available technologies and other processes, TSA determined that AIT is the most effective method to detect both metallic and non-metallic threat items concealed on passengers while maintaining efficient checkpoint screening operations. Our work with AIT began over three years ago, and has included testing and evaluation in both the laboratory and in airports. AIT represents the very latest in passenger screening technological advancement and addresses a broad range of threats. TSA tested and piloted the use of AIT at several airports around the country prior to the December 2009 attempted attack, and as a consequence, the agency was able to accelerate deployment of AIT following the incident to enable us to quickly and effectively detect metallic and non-metallic threats. Our extensive experience with AIT has made us the world leader in its implementation in the transportation environment.

According to TSA statistics, approximately one percent of passengers selected for AIT screening have opted out of AIT screening. Moreover, independent polls reflect that the traveling public supports these measures – for example, a recent CBS poll found four in five people approve of the use of AIT for screening, and a recent Gallup poll reported 78 percent of air travelers approve of the use of AIT at U.S. airports.

AIT is a Safe and Reliable Screening Technology

AIT machines are safe, efficient, and have built-in safeguards to protect passenger privacy. TSA requires its technology to comply with consensus-based scientific safety standards administered by the Health Physics Society and accredited by the American National Standards Institute.

The radiation dose from backscatter AIT machines has been independently evaluated by the Food and Drug Administration, the National Institute of Standards and Technology, and the Johns Hopkins University Applied Physics Laboratory, all of which have affirmed that the systems comply with established standards for safety. Public versions of our safety testing reports are available on TSA's website at www.tsa.gov.

A single screening using backscatter technology produces a radiation dose equivalent to approximately two minutes of flying on an airplane at altitude. Millimeter wave technology does not emit ionizing radiation and instead uses radio frequency energy. The energy projected by these units is a fraction of other commercially approved radio frequency devices, such as cell phones, two-way radios, and blue tooth devices.

TSA is Committed to Protecting Passenger Privacy

TSA has strict safeguards to protect passenger privacy and ensure anonymity. TSA's AIT machines deployed at airports do not store or print passenger images, and images are maintained on the monitor only for as long as it takes to resolve any anomalies. Images from TSA screening operations have not been and are not retained for any purpose. Additionally, the officer reviewing the image is unable to see the individual undergoing screening, and the officer screening the passenger cannot see the image – the image is completely disassociated with the passenger. Furthermore, AIT machines do not produce photographic quality images that would permit recognition of the person screened. TSA also applies facial blurs to both the millimeter wave and backscatter technologies.

The Chief Privacy Officer of the Department of Homeland Security (DHS) has conducted a Privacy Impact Assessment of the AIT machines and updated those assessments as the program has developed. The full results of that assessment are available to the public on the Privacy Office's website at www.dhs.gov/privacy. TSA's screening protocols ensure that such screening does not unreasonably intrude on a passenger's reasonable expectation of privacy in the airport environment and that the public's privacy concerns related to AIT screening are adequately addressed.

Automatic Target Recognition (ATR) To Further Address Privacy Concerns

While we are rapidly deploying AIT machines to U.S. airports, we also are exploring enhancements to this technology to further address privacy issues. To that end, we are field testing auto-detection software, referred to as Automatic Target Recognition (ATR), which enhances passenger privacy by eliminating passenger-specific images and instead highlights the area with a detected anomaly on a generic outline of a person. Pat downs used to resolve such anomalies will be limited to the areas of the body displaying an alarm unless the number of anomalies is sufficient to require a full-body pat down. If no anomalies are detected, the screen displays the word "OK" with no icon.

As with current AIT software, ATR-enabled units deployed at airports are not capable of storing or printing the generic image. This software eliminates the need for a remotely located TSO to view passenger images in a separate room because no actual image of the passenger is produced, reducing associated staffing and construction costs. ATR software represents a substantial step forward in addressing passenger privacy concerns, while maintaining TSA established standards for detection. TSA plans to continually update and test enhanced versions of the software in order to ensure technology with the highest detection standards is in use.

Employing Effective Pat Downs

TSA operates in a high-threat environment. Terrorists look for gaps or exceptions to exploit. They are studying our security measures and will exploit our social norms to their advantage. The device used in the December 25, 2009, bombing attempt illustrates this fact; it was cleverly constructed and intentionally hidden on a very sensitive part of the individual's body to avert detection by officials in Amsterdam. As a result, the lives of almost 300 passengers and crew were put at risk. My responsibility as TSA Administrator is to put in place reasonable security measures to counteract this and other types of threats.

Upon joining TSA in July 2010, I looked at the agency's efforts to address the threat posed by Umar Farouk Abdulmutallab's bombing attempt on December 25, 2009. I also considered several reports from the Government Accountability Office (GAO), DHS's Office of Inspector General (IG), and TSA's Office of Inspection, all of whom have performed a significant amount of covert testing of TSA's operations. One of the most significant findings of the covert testing was that pat downs were not thorough enough. The results of this repeated covert testing taken with the latest intelligence led to the conclusion that TSA needed to modify its pat-down procedures.

TSA will continue to work with the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office to ensure that TSA's pat-down procedures do not unduly impinge upon passengers' rights and liberties, and we will regularly reassess screening procedures to ensure they are set at an appropriate level to mitigate threats while protecting the passengers' privacy.

Implementing Secure Flight

As of November 23, 2010, TSA's Secure Flight program became fully operational for all covered flights operating to, from, and within the United States, fulfilling a key 9/11 Commission recommendation and increasing security by having TSA, rather than airlines, screen every passenger against the latest intelligence before a boarding pass is issued. Since its implementation, Secure Flight has demonstrated the value of uniform, consistent watch list matching through improved identification of matches. Continuous Secure Flight vetting begins 72 hours in advance of flight and continues until the flight departs, consistently providing insight into potential threats and enabling TSA to plan field efforts to counter any threat accordingly.

Collectively, there are 202 aircraft operators using Secure Flight, representing 100 percent of all aircraft operators covered by the Secure Flight Final Rule.

Advancing Air Cargo Security

TSA also continues to take aggressive action to improve the security of air cargo throughout the global air cargo network. In response to the October 2010 attempted bombings of cargo aircraft bound for the United States, TSA has issued security requirements restricting the transport of printer and toner cartridges, prohibiting elevated risk cargo from transport on passenger aircraft, requiring other cargo to undergo screening, and establishing requirements for handling international mail. In January 2011, TSA issued a proposed air carrier security program change to increase security measures for air cargo, most notably, to require 100 percent screening of inbound international cargo transported on passenger aircraft by December 31, 2011. TSA expects to finalize the programs in Spring 2011 after evaluating industry comments.

Additionally, as part of the DHS Air Cargo Security Working Group established by Secretary Napolitano, TSA is taking a leadership role in partnering with industry and other federal government partners to develop strategies to strengthen air cargo security while facilitating the flow of commerce. TSA is also working closely with U.S. Customs and Border Protection and the air cargo industry to receive and process pre-departure, advanced air cargo information from shippers earlier than is currently required so that we can increase the focus of our screening resources on high-threat cargo.

Reducing Surface Transportation Vulnerabilities

The Transportation Security Administration works with its partners in securing the surface transportation networks of the United States, working closely with transit agencies and state and local officials to assist them in defining and meeting their security requirements. The Transit Security Grant Program (TSGP) is a vital tool by which we enable and empower transit agency security providers to improve their practices. TSA works closely with the FEMA Grants Program Division to apply funding to projects with the most effective risk mitigation to the most at-risk transit properties. In 2010, the TSGP provided $273.4M to the transit industry and a total of $1.6B since 2006. Similar, but smaller grant programs have supported freight rail, over-the-road bus, and trucking programs.

TSA Surface Inspectors engage in all surface modes with activities ranging from inspecting rail yards and hazmat conveyances for regulatory compliance to assisting in the development of security and incident management plans. In the transit mode, the Surface Security Inspector program improves security by conducting field visits to assess the base line of security and subsequently developing action plans and assisting properties and agencies to improve their specific security programs. One such security program is the deployment of explosives detection canines, which are provided both through TSGP grant funding and appropriated TSA funds. TSA and the Department's Science and Technology Directorate are also partnering with Auburn University's well-regarded canine program to enhance the effectiveness of explosives detection canine teams used by TSA in protecting aviation and surface transportation by developing additional detection techniques and we welcome the opportunity to further brief the Subcommittee on these efforts.

TSA's VIPR teams are designed to enhance security by working in mass transit, aviation, rail and other transportation modes alongside local law enforcement agencies during specific times or events. VIPR teams are comprised of personnel with expertise in inspection, behavior detection, security screening, and law enforcement, and enhance TSA's ability to leverage a variety of resources quickly to increase security in any mode of transportation anywhere in the country. A component of TSA's nimble, unpredictable approach to security, TSA enhanced surface transportation security by conducting over 3,750 VIPR operations in 2010 in the various modes of surface transportation. VIPR operational plans are developed with a risk-based methodology, in conjunction with local transportation security stakeholders, and conducted jointly by TSA, local law enforcement, and transportation security resources.

TWIC Program Advancements

In the last two years, over 1.6 million workers have enrolled in the Transportation Worker Identification Credential (TWIC) program. The TWIC program includes a comprehensive security threat assessment, and the issuance of biometric credentials, which are now required to enter maritime facilities. TSA has processed 50,000 appeals and waiver requests, and continues to improve the adjudication process to shorten the time it takes to complete the security threat assessment process. After working through many challenges, TSA is concluding the TWIC Reader Pilot Program, wrapping up formal data collection, and working on the report to Congress. We continue to coordinate these efforts with the U.S. Coast Guard to ensure a high level of security and operational effectiveness.

Enhancing International Cooperation

The U.S. Government fully recognizes that it takes a concerted, global effort to protect the world's interconnected transportation networks. The security of U.S. civil aviation is intimately connected to the security of international civil aviation system writ large, and is directly affected by efforts that extend beyond our borders. For that reason, Secretary Napolitano and I have embarked on an aggressive outreach initiative to enhance civil aviation security standards and practices worldwide.

Immediately following the attempted bombing of a U.S.-bound Northwest Airlines flight on December 25, 2009, Secretary Napolitano began working with the International Civil Aviation Organization (ICAO) on an unprecedented global initiative to strengthen the international aviation system against the evolving threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry. Secretary Napolitano has participated in regional aviation security summits in Europe, South America, the Caribbean, Asia, and the Middle East, bringing about historic consensus with her international colleagues to strengthen the civil aviation system through improved information sharing, cooperation on technological development and enhanced aviation security standards.

These efforts culminated at the ICAO Triennial Assembly in October 2010, where the Assembly adopted the Declaration on Aviation Security, which highlights the commitment of the international community to collaborate in the effort to enhance aviation security at the international level. The extraordinary global collaboration demonstrated by the nearly 190 ICAO countries during the ICAO General Assembly in Montreal has helped to advance international security standards, broaden existing cooperation mechanisms and information exchange, and encourage the use of technology in the aviation security environment.

Specifically, following the Assembly, the ICAO Council adopted Amendment 12 to Annex 17 to the International Convention on Civil Aviation (also known as the Chicago Convention), which governs international civil aviation security. These amendments will tighten the existing international standards to account for new and emerging threats, and also establish enhanced standards for air cargo security. TSA will continue its work to further enhance international security standards vis-à-vis evolving threats and risk of unlawful interference with civil aviation.

Further, throughout 2010, DHS and TSA played a significant role in developing the ICAO Comprehensive Aviation Security Strategy, also adopted at the ICAO Assembly in October 2010, which sets the course for ICAO's aviation security efforts over the next six years. This strategy establishes seven key focus areas, which are built upon DHS/TSA's strategic goals for the enhancement of international aviation. These include addressing new and emerging threats; promoting innovative, effective and efficient security approaches; promoting the sharing of information amongst member states to raise awareness of threats and security trends relevant to civil aviation operations; promoting global compliance and establishing sustainable aviation security oversight; improving human factors and security culture; promoting the development of mutual recognition for aviation security processes; and emphasizing the importance of security.

Lastly, senior DHS leadership from the Private Sector Office, TSA and CBP began collaboratively engaging with the aviation industry in a dialogue about security changes, a practice that we will continue regularly this year.

Continuing Engagement

TSA is actively involved in various bilateral Transportation and Aviation Security Working Groups, and is an active participant in regional and multilateral organizations such as the G8, the Asia-Pacific Economic Cooperation, the Quadrilateral Group on Transportation Security, and the ICAO Regional Offices. Furthermore, TSA has been actively reaching out to other regional organizations such as the Latin American Civil Aviation Conference, the Arab Civil Aviation Conference, the Central American Corporation for Air Navigation Services, and the African Civil Aviation Conference and the African Union. Through these forums, TSA is able to encourage and assist in the enhancement of international aviation security standards and practices, and to better understand the legal, political, cultural, geographic, and operational issues that may affect our foreign partners' ability to address certain aviation security. Finally, this past November, TSA hosted an international policy summit on AIT at TSA's Systems Integration Facility, which brought together key policy makers and experts from over 30 countries and 11 industry associations to discuss and exchange views on AIT. Discussions centered on legal, policy, privacy, operational, and health, safety and science aspects of AIT and the deployment of such screening capability at airports in different locations around the world.

TSA, in conjunction with the Department of State, is also working with foreign governments to gain their acceptance of Federal Air Marshals on international flights to and from more countries. This expansion of covered flights will further enhance aviation security for passengers and aircraft.

Conclusion

I want to thank the subcommittee for its continued assistance to TSA and for the opportunity to discuss these important issues of transportation security. I am pleased to answer any questions you might have.